Kyle McLean (SBN #330580)
Email: kmclean@sirillp.com
Mason Barney*
Email: mbarney@sirillp.com
Tyler Bean*
Email: tbean@sirillp.com
SIRI & GLIMSTAD LLP
700 S. Flower Street, Ste. 1000
Los Angeles, CA 90017
Telephone: 213-376-3739

Attorneys for Plaintiff and the Nationwide Class

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

KERRY LAMONS and **TANEISHA ROBERTSON**, individually and on behalf of her minor children, **X.R.** and **J.R.**, and all others similarly situated, Plaintiffs, v. **DELTA DENTAL OF CALIFORNIA and DELTA DENTAL INSURANCE COMPANY,** Defendants.	Case No. JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiffs Kerry Lamons and Taneisha Robertson ("Plaintiffs"), individually and on behalf of her minor children, X.R. and J.R., and all similarly situated persons,

allege the following against Delta Dental of California and Delta Dental Insurance Company ("DDIC") (collectively referred to herein as "Delta Dental" or "Defendant") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by their counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. Plaintiffs bring this class action against Delta Dental for its failure to properly secure and safeguard Plaintiffs' and other similarly situated Delta Dental members' personally identifiable information ("PII") and protected health information ("PHI"), including dates of birth, Social Security numbers, passport numbers, financial account details, tax identification numbers, and health insurance and health information[1] (the "Private Information"), from criminal hackers.

2. Delta Dental, based in San Francisco, is a dental insurance company that serves more than 6,928,932 customers throughout the United States.

3. On or about December 14, 2023, Delta Dental filed official notice of a hacking incident with the Office of the Maine Attorney General.[2] Under state and federal law, organizations must report breaches involving PHI within at least sixty (60) days.

[1] *See* https://www.securityweek.com/delta-dental-of-california-discloses-data-breach-impacting-6-9-million-people/ (last visited on January 2, 2024).
[2] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/0f821b31-9e4f-4b15-872c-69fef62a93fa.shtml (last visited Jan. 2, 2024).

4. On or about December 15, 2023, Delta Dental also sent out data breach letters (the "Notice") to individuals whose information was compromised as a result of the hacking incident.

5. Based on the Notice sent to Plaintiffs and "Class Members" (defined below), on June 1, 2023, Defendants learned that their file transfer vendor, MOVEit, experienced a cyber-attack. In response, Defendants stopped access to the MOVEit software and launched an investigation. On July 6, 2023, Defendants' investigation confirmed that an unauthorized party had access to certain files that contained sensitive member information, and that such access took place between May 27, 2023, and May 30, 2023 (the "Data Breach"). Yet, Delta Dental waited more than *five months* to notify the public that they were at risk, despite its non-delegable legal obligations to do so much sooner.

6. As a result of this delayed response, Plaintiffs and Class Members had no idea for *five months* that their Private Information had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

7. The Private Information compromised in the Data Breach contained highly sensitive member data that Delta Dental collected and maintained, representing a gold mine for data thieves.

8. Armed with the Private Information accessed in the Data Breach (and a head start), data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, and filing fraudulent tax returns.

9. There has been no assurance offered by Delta Dental that all personal data or copies of data have been recovered or destroyed, or that Defendants have adequately enhanced their data security practices sufficiently to avoid a similar breach in the future.

10. Therefore, Plaintiffs and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering, ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their Private Information, the loss of the benefit of their bargain, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

11. Plaintiffs bring this class action lawsuit to address Delta Dental's inadequate safeguarding of Class Members' Private Information that they collected and maintained, and their failure to provide timely and adequate notice to Plaintiffs and Class Members of the types of information that were accessed, and that such information was subject to unauthorized access by cybercriminals.

12. The potential for improper disclosure and theft of Plaintiffs' and Class Members' Private Information was a known risk to Delta Dental, and thus Delta Dental was on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

13. Upon information and belief, Delta Dental failed to properly monitor and implement proper security practices regarding the computer network and systems that housed the Private Information. Had Delta Dental properly monitored the networks housing their members' Private Information, they could have prevented the Data Breach, or at least discovered it sooner.

14. Plaintiffs' and Class Members' identities are now at risk because of Delta Dental's negligent conduct as the Private Information that Delta Dental collected and maintained is now in the hands of data thieves and other unauthorized third parties.

15. Plaintiffs seek to remedy these harms on behalf of themselves, Plaintiff Robertson's minor children, and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

16. Accordingly, Plaintiffs, on behalf of themselves, Plaintiff Robertson's minor children, and the Class, assert claims for Negligence, Breach of Contract, Breach of Implied Contract, Unjust Enrichment/Quasi-Contract, Breach of Fiduciary Duty, and Declaratory Judgment/Injunctive Relief.

17. Plaintiff Lamons, on behalf of herself and the "California Subclass" (defined below), also asserts claims for Violation of California's Confidentiality of Medical Information Act and Unfair Competition Act.

II. PARTIES

18. Plaintiff Taneisha Robertson is, and at all times mentioned herein was, an individual citizen of the State of Georgia.

19. Plaintiff Kerry Lamons is, and at all times mentioned herein was, an individual citizen of the State of California.

20. Defendant Delta Dental of California is a dental insurance company incorporated in California, with its principal place of business at 560 Mission Street Suite 1300, San Francisco, California, 94105.

21. Defendant Delta Dental Insurance Company is a Delaware Corporation with its principal place of business at 560 Mission Street, #1300, San Francisco, CA 94105. DDIC represents that it offers and administers Delta Dental PPO and other fee-for-service dental programs in Alabama, Florida, Georgia, Louisiana, Mississippi, Montana, Nevada, and Utah.

III. JURISDICTION AND VENUE

22. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the

number of class members is over 100, many of whom have different citizenship from Delta Dental. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

23. This Court has jurisdiction over Delta Dental because Delta Dental operates in and/or is incorporated in this District.

24. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District and Delta Dental has harmed Class Members residing in this District.

IV. FACTUAL ALLEGATIONS

A. Delta Dental's Business and Collection of Plaintiffs' and Class Members' Private Information

25. Delta Dental is a dental insurance provider. Founded in 1955, Delta Dental of California is a part of a larger network of companies known as "Delta Dental Plans Association" which serves millions of members throughout the United States. Upon information and belief, Delta Dental employs more than 2,925 people and generates approximately $5 billion in revenue.

26. As a condition of receiving dental insurance, Delta Dental requires that its members entrust it with highly sensitive personal and health information. In the ordinary course of receiving service from Delta Dental, Plaintiffs and Class Members were required to provide their Private Information to Defendants.

27. In their Notice of Privacy Practices, Delta Dental informs its members that it is "required by law to maintain the privacy and security of your Protected

Health Information (PHI)."[3] Delta Dental describes in their Privacy Policy the limited specific instances when they share member health information and says that they "will not use or disclose your PHI without your prior written authorization."[4] Delta Dental also states that: "Any third-party affiliates performing services on our behalf has signed a contract agreeing to protect the confidentiality of your PHI and has implemented privacy policies and procedures that comply with applicable federal and state law."[5]

28. Thus, due to the highly sensitive and personal nature of the information Delta Dental acquires and stores with respect to its members, Delta Dental, upon information and belief, promises to, among other things: keep members' Private Information private; comply with industry standards related to data security and the maintenance of their members' Private Information; inform members of their legal duties relating to data security and comply with all federal and state laws protecting members' Private Information; only use and release members' Private Information for reasons that relate to the services they provide; and provide adequate notice to members if their Private Information is disclosed without authorization.

29. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Delta Dental assumed legal and equitable

[3] See https://www1.deltadentalins.com/about/legal/privacy/hipaa-privacy.html (last visited Jan. 2, 2024).
[4] *Id.*
[5] *Id.*

duties they owed to them and knew or should have known that they are responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure and exfiltration.

30. Plaintiffs and Class Members relied on Delta Dental to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this Information, which Defendants ultimately failed to do.

B. The Data Breach and Defendants' Inadequate Notice to Plaintiffs and Class Members

31. According to Defendants' Notice, they "learned unauthorized actors exploited a vulnerability affecting the MOVEit file transfer software application" on June 1, 2023. After conducting an investigation, Defendants confirmed on July 6, 2023, that their members' information stored on its MOVEit platform "had been accessed and acquired without authorization between May 27, 2023, and May 30, 2023."

32. Through the Data Breach, the unauthorized cybercriminal(s) accessed a cache of highly sensitive Private Information from Defendants, including Plaintiffs' and Class Members' Social Security numbers, health information, and health insurance information.

33. On or about December 15, 2023, roughly *five months* after Delta Dental learned that the Class's Private Information was first accessed by cybercriminals, Delta Dental finally began to notify their members of the Data Breach.

34. Delta Dental had non-delegable duties and obligations created by statute, contract, industry standards, common law, and representations made to Plaintiffs and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

35. Plaintiffs and Class Members provided their Private Information to Delta Dental with the reasonable expectation and mutual understanding that Delta Dental would comply with their obligations to keep such Information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

36. Delta Dental's data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

37. Delta Dental knew or should have known that their members' electronic records would be targeted by cybercriminals.

C. The Healthcare Sector is Particularly Susceptible to Data Breaches

38. Delta Dental was on notice that companies in the healthcare industry are susceptible targets for data breaches.

39. Delta Dental was also on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the

purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PHI)."[6]

40. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their members' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[7]

41. The healthcare sector reported the second largest number of data breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[8] In 2022, the largest growth in compromises occurred in the healthcare sector.[9]

---

[6] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, Reuters (Aug. 2014), *available at* https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last visited on Jan. 2, 2024).

[7] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass'n. (Oct. 4, 2019), *available at*: https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last visited on Jan. 2, 2024).

[8] Identity Theft Resource Center, *2018 End-of-Year Data Breach Report, available at*: https://www.idtheftcenter.org/2018-data-breaches/ (last visited on Jan. 2, 2024).

[9] Identity Theft Resource Center, *2022 End-of-Yeare Data Breach Report, available at*: https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf (last visited on Jan. 2, 2024).

42. Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident … came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[10]

43. Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[11]

44. Healthcare related breaches have continued to rapidly increase because electronic PHI is seen as a valuable asset. "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[12]

---

[10] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), *available at:* https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/ (last visited on Jan. 2, 2024).

[11] *Id*.

[12] Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, *available at*: https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last visited on Jan. 2, 2024).

45. As a provider health insurance and healthcare related services, Delta Dental knew, or should have known, the importance of safeguarding their members' Private Information, including PHI, entrusted to them, and of the foreseeable consequences if such data were to be disclosed. These consequences include the significant costs that would be imposed on Delta Dental's members as a result of a breach. Delta Dental failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

D. Delta Dental Failed to Comply with HIPAA

46. Title II of HIPAA contains what are known as the Administration Simplification provisions. *See* 42 U.S.C. §§ 1301, *et seq*. These provisions require that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PHI similar to the data Defendants left unguarded and vulnerable to attack. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

47. Delta Dental's Data Breach resulted from a combination of insufficiencies that indicate Delta Dental failed to comply with safeguards mandated by HIPAA regulations and industry standards. First, it can be inferred from Delta Dental's Data Breach that Delta Dental either failed to implement, or inadequately implemented, information security policies or procedures to protect Plaintiffs' and Class Members' PHI.

48. Plaintiffs' and Class Members' Private Information compromised in the Data Breach included "protected health information" as defined by CFR § 160.103.

49. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

50. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

51. Plaintiffs' and Class Members' Private Information included "unsecured protected health information" as defined by 45 CFR § 164.402.

52. Plaintiffs' and Class Members' unsecured PHI was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

53. Based upon Defendants' Notice to Plaintiffs and Class Members, Delta Dental reasonably believes that Plaintiffs' and Class Members' unsecured PHI has been acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

54. Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart

E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

55. Delta Dental reasonably believes that Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

56. Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

57. Plaintiffs' and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach.

58. Delta Dental reasonably believes that Plaintiffs' and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach.

59. It is reasonable to infer that Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

60. It should be rebuttably presumed that unsecured PHI acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

61. After receiving notice that they were victims of the Data Breach (which required the filing of a data breach report in accordance with 45 CFR § 164.408(a)), it is reasonable for recipients of that notice, including Plaintiffs and Class Members in this case, to believe that future harm (including medical identity theft) is real and imminent, and to take steps necessary to mitigate that risk of future harm.

62. In addition, Delta Dental's Data Breach could have been prevented if Delta Dental had implemented HIPAA mandated, industry standard policies and procedures for securely disposing of PHI when it was no longer necessary and/or had honored their obligations to their members.

63. Delta Dental's security failures also include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality and integrity of electronic protected health information Delta Dental creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

f. Failing to identify and respond to suspected or known security incidents;

g. Failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii);

h. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2);

i. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3);

j. Failing to ensure compliance with HIPAA security standard rules by Defendants' workforce, in violation of 45 CFR 164.306(a)(94); and

k. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

64. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414 also required Delta Dental to provide notice of the Data Breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***" (emphasis added).

65. Because Delta Dental has failed to comply with HIPAA, while monetary relief may cure some of Plaintiffs' and Class Members' injuries, injunctive relief is also necessary to ensure Delta Dental's approach to information security is adequate and appropriate going forward. Delta Dental still maintains the PHI and other highly sensitive PII of their current and former members, including Plaintiffs and Class Members. Without the supervision of the Court through injunctive relief, Plaintiffs' and Class Members' Private Information remains at risk of subsequent data breaches.

E. Delta Dental Failed to Comply with FTC Guidelines

66. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be

factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

67. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

68. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

69. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

70. As evidenced by the Data Breach, Delta Dental failed to properly implement basic data security practices. Delta Dental's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

71. Defendants were at all times fully aware of their obligation to protect the Private Information of their members yet failed to comply with such obligations. Defendants were also aware of the significant repercussions that would result from their failure to do so.

F. Delta Dental Failed to Comply with Industry Standards

72. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

73. Some industry best practices that should be implemented by businesses dealing with sensitive PHI like Delta Dental include but are not limited to educating

all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendants failed to follow some or all of these industry best practices.

74. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendants failed to follow these cybersecurity best practices.

75. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

76. Defendants failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

G. Delta Dental Breached their Duty to Safeguard Plaintiffs' and Class Members' Private Information

77. In addition to their obligations under federal and state laws, Delta Dental owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information entrusted to them from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Delta Dental owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their vendor's computer systems, networks, and protocols adequately protected the Private Information of Class Members

78. Delta Dental breached their obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because they failed to properly maintain and safeguard the computer systems that housed their members' data. Delta Dental's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect members' Private Information;

c. Failing to properly monitor their data security systems for existing intrusions;

d. Failing to sufficiently train their employees regarding the proper handling of their members Private Information;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

f. Failing to adhere to HIPAA and industry standards for cybersecurity as discussed above; and

g. Otherwise breaching their duties and obligations to protect Plaintiffs' and Class Members' Private Information.

79. Delta Dental negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access the computer network and systems which contained unsecured and unencrypted Private Information.

80. Had Delta Dental remedied the deficiencies in their vendor's information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, they could have prevented intrusion into the information storage and security systems and, resultant, theft of Plaintiffs' and Class Members' confidential Private Information.

81. Accordingly, Plaintiffs' and Class Members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, fraud

and identity theft. Plaintiffs and Class Members also lost the benefit of the bargain they made with Delta Dental.

H. Delta Dental Should Have Known that Cybercriminals Target PII and PHI to Carry Out Fraud and Identity Theft

82. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiffs and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[13] Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

83. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

[13] *FTC Information Injury Workshop, BE and BCP Staff Perspective,* Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited on Jan. 2, 2024).

84. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

85. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

86. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiffs' and Class Members' Private Information to access accounts, including, but not limited to, email accounts

and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiffs and Class Members.

87. One such example of this is the development of "Fullz" packages.

88. Cybercriminals can cross-reference two sources of the Private Information compromised in the Data Breach to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

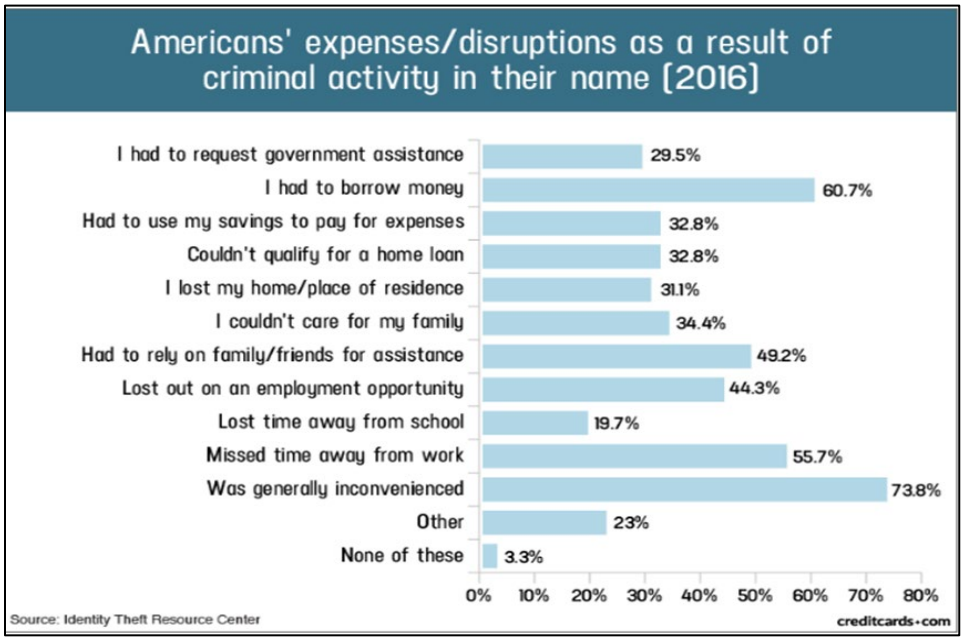
89. The development of "Fullz" packages means that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and the proposed Class's phone numbers, email addresses, and other sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card or financial account numbers may not be included in the Private Information stolen in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs and other Class Members' stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

90. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[14] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

91. Identity thieves can also use stolen personal information such as Social Security numbers and PHI for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return or insurance claim using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number or receive medical services in the victim's name.

[14] *See IdentityTheft.gov,* Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited Jan. 2, 2024).

92. In fact, a study by the Identity Theft Resource Center[15] shows the multitude of harms caused by fraudulent use of PII:



93. PHI is also especially valuable to identity thieves. As the FTC recognizes, identity thieves can use PHI to commit an array of crimes, including identity theft and medical and financial fraud.[16]

94. Indeed, a robust cyber black market exists in which criminals openly post stolen PHI on multiple underground Internet websites, commonly referred to as the dark web.

[15] Steele, Jason, *Credit Card, and ID Theft Statistics*, CreditCards.com (October 23, 2017), *available at* https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/ (last visited on Jan. 2, 2024).

[16] Federal Trade Commission, *Warning Signs of Identity Theft, available at*: https://consumer.ftc.gov/articles/what-know-about-identity-theft (last visited on Jan. 2, 2024).

95. While credit card information and associated PII can sell for as little as $1-$2 on the black market, protected health information can sell for as much as $363 according to the Infosec Institute.[17]

96. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

97. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[18]

[17] Center for Internet Security, *Data Breaches: In the Healthcare Sector, available at*: https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector (last visited on Jan. 2, 2024).

[18] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, *available at*: https://kffhealthnews.org/news/rise-of-indentity-theft/ (last visited on Jan. 2, 2024).

98. The ramifications of Delta Dental's failure to keep their members' Private Information secure are long-lasting and severe. Once it is stolen, fraudulent use of such and damage to victims may continue for years.

99. Here, not only was sensitive medical information compromised, but Social Security numbers were compromised too. The value of both PII and PHI is axiomatic. The value of "big data" in corporate America is astronomical. The fact that identity thieves attempt to steal identities notwithstanding possible heavy prison sentences illustrates beyond a doubt that the Private Information compromised here has considerable market value.

100. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or PHI is stolen and when it is misused. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[19]

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data [has] been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

[19] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), *available at* https://www.gao.gov/assets/270/262904.html (last visited Jan. 2, 2024).

101. PII and PHI are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the dark web for years.

102. As a result, Plaintiffs and Class Members are at an increased risk of fraud and identity theft, including medical identity theft, for many years into the future. Thus, Plaintiffs and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

I. Plaintiffs' and Class Members' Damages

Plaintiff Robertson's Experience

103. When Plaintiff Robertson became a member and recipient of Defendants' services, Defendants required Plaintiff Robertson provide it with substantial amounts of her and her minor children's Private Information, including PHI.

104. On or about December 15, 2023, Plaintiff Robertson received a letter entitled "Notice of Data Security Incident" which told her that her Private Information along with her minor children's Private Information had been accessed and acquired during the Data Breach. The notice letter informed her that the Private Information stolen included her "date of birth, Social Security number, and health insurance information."

105. The notice letter offered Plaintiff Robertson only two years of credit monitoring services. Two years of credit monitoring is not sufficient given that Plaintiff Robertson will now experience a lifetime of increased risk of identity theft, including but not limited to, potential medical fraud.

106. Plaintiff Robertson suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring her accounts for fraud.

107. Plaintiff Robertson would not have provided her Private Information to Defendants had Defendants timely disclosed that they lacked adequate computer and data security practices to safeguard their members' personal and health information from theft, and that those systems were subject to a data breach.

108. Plaintiff Robertson suffered actual injury in the form of having her PII and PHI compromised and/or stolen as a result of the Data Breach.

109. Plaintiff Robertson suffered actual injury in the form of damages to and diminution in the value of her personal, health, and financial information – a form of intangible property that Plaintiff Robertson entrusted to Defendants for the purpose of receiving healthcare services from them, which was compromised in, and as a result of, the Data Breach.

110. Plaintiff Robertson suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by her Private Information being placed in the hands of criminals.

111. Plaintiff Robertson has a continuing interest in ensuring that her PII and PHI, which remain in the possession of Defendants, are protected, and safeguarded from future breaches.

112. As a result of the Data Breach, Plaintiff Robertson made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and researching the credit monitoring offered by Defendants. Plaintiff Robertson has spent several hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities.

113. As a result of the Data Breach, Plaintiff Robertson has suffered anxiety as a result of the release of her PII and PHI, which she believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using her PII and PHI for purposes of committing cyber and other crimes against her including, but not limited to, fraud and identity theft. Plaintiff Robertson is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach would have on her life.

114. Plaintiff Robertson also suffered actual injury from having her Private Information compromised as a result of the Data Breach in the form of (a) damage to and diminution in the value of her PII and PHI, a form of property that Defendants obtained from Plaintiff Robertson; (b) violation of her privacy rights; and (c) present,

imminent, and impending injury arising from the increased risk of identity theft, and fraud she now faces.

115. As a result of the Data Breach, Plaintiff Robertson anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Breach.

Plaintiff Kerry Lamons' Experience

116. When Plaintiff Lamons became a member and recipient of Defendants' services, Defendants required Plaintiff Lamons provide them with substantial amounts of her Private Information, including PHI.

117. On or about December 15, 2023, Plaintiff Lamons received a letter entitled "Notice of Data Security Incident" which told her that her Private Information had been accessed and acquired during the Data Breach.

118. The notice letter offered Plaintiff Lamons only two years of credit monitoring services. Two years of credit monitoring is not sufficient given that Plaintiffs Lamons will now experience a lifetime of increased risk of identity theft, including but not limited to, potential medical fraud.

119. Plaintiff Lamons suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring her accounts for fraud.

120. Plaintiff Lamons would not have provided her Private Information to Defendants had Defendants timely disclosed that they lacked adequate computer and

data security practices to safeguard their members' personal and health information from theft, and that those systems were subject to a data breach.

121. Plaintiff Lamons suffered actual injury in the form of having her PII and PHI compromised and/or stolen as a result of the Data Breach.

122. Plaintiff Lamons suffered actual injury in the form of damages to and diminution in the value of her personal, health, and financial information – a form of intangible property that Plaintiff Lamons entrusted to Defendants for the purpose of receiving healthcare services from them, which was compromised in, and as a result of, the Data Breach.

123. Plaintiff Lamons suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by her Private Information being placed in the hands of criminals.

124. Plaintiff Lamons has a continuing interest in ensuring that her PII and PHI, which remain in the possession of Defendants, are protected, and safeguarded from future breaches.

125. As a result of the Data Breach, Plaintiff Lamons made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and researching the credit monitoring offered by Defendants. Plaintiff Lamons has spent several hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities.

126. As a result of the Data Breach, Plaintiff Lamons has suffered anxiety as a result of the release of her PII and PHI, which she believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using her PII and PHI for purposes of committing cyber and other crimes against her including, but not limited to, fraud and identity theft. Plaintiff Lamons is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach would have on her life.

127. Plaintiff Lamons also suffered actual injury from having her Private Information compromised as a result of the Data Breach in the form of (a) damage to and diminution in the value of her PII and PHI, a form of property that Defendants obtained from Plaintiff Lamons; (b) violation of her privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud she now faces.

128. As a result of the Data Breach, Plaintiff Lamons anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Breach.

129. In sum, Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

130. Plaintiffs and Class Members entrusted their Private Information to Defendants in order to receive Defendants' services.

131. Their Private Information was subsequently compromised as a direct and proximate result of the Data Breach, which Data Breach resulted from Defendants' inadequate data security practices.

132. As a direct and proximate result of Delta Dental's actions and omissions, Plaintiffs and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having medical services billed in their names, loans opened in their names, tax returns filed in their names, utility bills opened in their names, credit card accounts opened in their names, and other forms of identity theft.

133. Further, and as set forth above, as a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have also been forced to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

134. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

135. Plaintiffs and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the

misuse of their Private Information, since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiffs and Class Members.

136. The Private Information maintained by and stolen from Defendants' systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiffs and Class Members, which can also be used to carry out targeted fraudulent schemes against Plaintiffs and Class Members.

137. Plaintiffs and Class Members also lost the benefit of the bargain they made with Delta Dental. Plaintiffs and Class Members overpaid for services that were intended to be accompanied by adequate data security but were not. Indeed, part of the price Plaintiffs and Class Members paid to Delta Dental was intended to be used by Delta Dental to fund adequate security of Delta Dental's systems to protect Plaintiffs' and Class Members' Private Information. Thus, Plaintiffs and the Class did not receive the benefit of the bargain.

138. Additionally, Plaintiffs and Class Members also suffered a loss of value of their PII and PHI when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[20] In fact,

[20] *See* https://thequantumrecord.com/blog/data-brokers-profit-from-our-data/#:~:text=The%20business%20of%20data%20brokering,annual%20revenue%20of%20%24200%20billion. (last visited on Jan. 2, 2024).

consumers who agree to provide their web browsing history to the Nielsen Corporation can in turn receive up to $50 a year.[21]

139. As a result of the Data Breach, Plaintiffs', and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has been harmed and diminished due to its acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is apparently readily available to others, and the rarity of the Private Information has been destroyed because it is no longer only held by Plaintiffs and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiffs and the Class Members, thereby causing additional loss of value.

140. Finally, Plaintiffs and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

141. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of Delta Dental, is protected from future breaches by the implementation of more adequate

---

[21] *Frequently Asked Questions,* Nielsen Computer & Mobile Panel, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited on Jan. 2, 2024).

data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing highly sensitive personal and health information of their members is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

142. As a direct and proximate result of Delta Dental's actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

V. CLASS ACTION ALLEGATIONS

143. Plaintiffs bring this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

144. Specifically, Plaintiffs propose the following "Nationwide Class" and "California Subclass" (collectively referred to herein as the "Class" or "Classes"), subject to amendment as appropriate:

Nationwide Class

All individuals, including minor children, in the United States who had Private Information accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach.

California Subclass

All living individuals, including minor children, residing in California who had Private Information accessed and/or

acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach.

145. Excluded from the Class are Defendants and their parents or subsidiaries, any entities in which they have a controlling interest, as well as their officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

146. Plaintiffs reserve the right to modify or amend the definitions of the proposed Nationwide Class, as well as the California Subclass, before the Court determines whether certification is appropriate.

147. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

148. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of 6,928,932 members of Delta Dental whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through Delta Dental's records, Class Members' records, publication notice, self-identification, and other means.

149. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Delta Dental engaged in the conduct alleged herein;

b. Whether Delta Dental's conduct violated the FTCA and HIPAA;

c. When Delta Dental learned of the Data Breach;

d. Whether Delta Dental's response to the Data Breach was adequate;

e. Whether Delta Dental unlawfully lost or disclosed Plaintiffs' and Class Members' Private Information;

f. Whether Delta Dental failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

g. Whether Delta Dental's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

h. Whether Delta Dental's data security systems prior to and during the Data Breach were consistent with industry standards;

i. Whether Delta Dental owed a duty to Class Members to safeguard their Private Information;

j. Whether Delta Dental breached their duty to Class Members to safeguard their Private Information;

k. Whether hackers obtained Class Members' Private Information via the Data Breach;

l. Whether Delta Dental had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and the Class Members;

m. Whether Delta Dental breached their duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

n. Whether Delta Dental knew or should have known that their data security systems and monitoring processes were deficient;

o. What damages Plaintiffs and Class Members suffered as a result of Delta Dental's misconduct;

p. Whether Delta Dental's conduct was negligent;

q. Whether Delta Dental was unjustly enriched;

r. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

s. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

150. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiffs' claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of Delta Dental. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other Class Members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of Class Members arise from the same operative facts and are based on the same legal theories.

151. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

152. Predominance. Delta Dental has engaged in a common course of conduct toward Plaintiffs and Class Members in that all of Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Delta Dental's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

153. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Delta Dental. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

154. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Delta Dental has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

155. Finally, all members of the proposed Class are readily ascertainable. Delta Dental has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Delta Dental.

VI. CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

156. Plaintiffs restate and reallege all of the allegations stated above as if fully set forth herein.

157. Delta Dental knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

158. Delta Dental's duty also included a responsibility to implement processes by which they could detect and analyze a breach quickly to give prompt notice to those affected in the case of a cyberattack.

159. Delta Dental knew or should have known of the risks inherent in collecting the Private Information of Plaintiffs and Class Members and the importance of adequate security. Delta Dental was on notice because, on information and belief, they knew or should have known that member information would be an attractive target for cyberattacks.

160. Delta Dental owed a duty of care to Plaintiffs and Class Members whose Private Information was entrusted to them. Delta Dental's duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in their possession;

b. To protect members' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in their possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiffs and Class Members pursuant to HIPAA and the FTCA;

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. To promptly notify Plaintiffs and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

161. Delta Dental's duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which

prohibits "unfair . . . practices in or affecting commerce," including, as interpreted, and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

162. Delta Dental's duty also arose because they are bound by industry standards to protect their members' confidential Private Information.

163. Plaintiffs and Class Members were foreseeable victims of any inadequate security practices on the part of Defendants, and Delta Dental owed them a duty of care to not subject them to an unreasonable risk of harm.

164. Delta Dental, through their actions and/or omissions, unlawfully breached their duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Private Information within Delta Dental's possession.

165. Delta Dental, by their actions and/or omissions, breached their duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiffs and Class Members.

166. Delta Dental, by their actions and/or omissions, breached their duty of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

167. Delta Dental breached their duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of the networks and systems that housed their members' Private Information;

c. Allowing unauthorized access to Class Members' Private Information;

d. Failing to comply with the FTCA;

e. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

f. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

168. Delta Dental acted with reckless disregard for the rights of Plaintiffs and Class Members by failing to provide prompt and adequate individual notice of the Data Breach such that Plaintiffs and Class Members could take measures to protect themselves from damages caused by the fraudulent use of the Private Information compromised in the Data Breach.

169. Delta Dental had a special relationship with Plaintiffs and Class Members. Plaintiffs' and Class Members' willingness to entrust Delta Dental with their Private Information was predicated on the understanding that Delta Dental would take adequate security precautions. Moreover, Delta Dental had the ability to protect the Private Information in their possession from attack.

170. Delta Dental's breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' Private Information to be compromised and exfiltrated as alleged herein.

171. Delta Dental's breach of duty also caused a substantial, imminent risk to Plaintiffs and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

172. As a result of Delta Dental's negligence in breach of their duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

173. Delta Dental also had independent duties under state law that required it to reasonably safeguard Plaintiffs' and Class Members' Private Information and promptly notify them about the Data Breach.

174. As a direct and proximate result of Delta Dental's negligent conduct, Plaintiffs and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

175. The injury and harm that Plaintiffs and Class Members suffered was reasonably foreseeable.

176. Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

177. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring Delta Dental to, *inter alia*, strengthen their data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT II
BREACH OF CONTRACT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

178. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

179. Plaintiffs and Class Members entered into a valid and enforceable contract through which they paid money to Delta Dental in exchange for services. That contract included promises by Defendants to secure, safeguard, and not disclose Plaintiffs' and Class Members' Private Information.

180. Delta Dental's Privacy Policy memorialized the rights and obligations of Delta Dental and their members. This document was provided to Plaintiffs and Class Members in a manner in which it became part of the agreement for services.

181. In the Privacy Policy, Delta Dental commits to protecting the privacy and security of private information and promises to never share Plaintiffs' and Class Members' Private Information except under certain limited circumstances.

182. Plaintiffs and Class Members fully performed their obligations under their contracts with Delta Dental.

183. However, Delta Dental did not secure, safeguard, and/or keep private Plaintiffs' and Class Members' Private Information, and therefore Delta Dental breached their contracts with Plaintiffs and Class Members.

184. Delta Dental allowed third parties to access, copy, and/or exfiltrate Plaintiffs' and Class Members' Private Information without permission. Therefore, Delta Dental breached the Privacy Policy with Plaintiffs and Class Members.

185. Delta Dental's failure to satisfy their confidentiality and privacy obligations, specifically those arising under the FTCA, HIPAA, and applicable industry standards, resulted in Delta Dental providing services to Plaintiffs and Class Members that were of a diminished value.

186. As a result, Plaintiffs and Class Members have been harmed, damaged, and/or injured as described herein, including in Defendants' failure to fully perform their part of the bargain with Plaintiffs and Class Members.

187. As a direct and proximate result of Delta Dental's conduct, Plaintiffs and Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

188. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring Delta Dental to, *inter alia*, strengthen their data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT III
BREACH OF IMPLIED CONTRACT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

189. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

190. This Count is pleaded in the alternative to Count III above.

191. Delta Dental provides dental insurance to Plaintiffs and Class Members. Plaintiffs and Class Members formed an implied contract with Defendants regarding the provision of those services through their collective conduct, including by Plaintiffs and Class Members paying for services and/or entrusting their valuable Private Information to Defendants in exchange for such services.

192. Through Defendants' sale of services to Plaintiffs and Class Members, they knew or should have known that they must protect Plaintiffs' and Class Members' confidential Private Information in accordance with their policies, practices, and applicable law.

193. As consideration, Plaintiffs and Class Members paid money to Delta Dental and/or turned over valuable Private Information to Delta Dental.

Accordingly, Plaintiffs and Class Members bargained with Delta Dental to securely maintain and store their Private Information.

194. Delta Dental accepted payment and/or possession of Plaintiffs' and Class Members' Private Information for the purpose of providing services to Plaintiffs and Class Members.

195. In paying Defendants and/or providing their valuable Private Information to Defendants in exchange for Defendants' services, Plaintiffs and Class Members intended and understood that Delta Dental would adequately safeguard the Private Information as part of those services.

196. Defendants' implied promises to Plaintiffs and Class Members include, but are not limited to, (1) taking steps to ensure that anyone who is granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the Private Information that is placed in the control of their employees is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained employees and/or agents; (4) designing and implementing appropriate retention policies to protect the Private Information against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; (7) complying with HIPAA standards to make sure that Plaintiffs' and Class Members' PHI would remain protected; and (8) taking other steps to protect against foreseeable data breaches.

197. Plaintiffs and Class Members would not have entrusted their Private Information to Delta Dental in the absence of such an implied contract.

198. Had Delta Dental disclosed to Plaintiffs and the Class that they did not have adequate computer systems and security practices to secure sensitive data, Plaintiffs and Class Members would not have provided their Private Information to Delta Dental.

199. As a provider of healthcare, Delta Dental recognized (or should have recognized) that Plaintiffs' and Class Member's Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain with Plaintiffs and the other Class Members.

200. Delta Dental violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiffs' and Class Members' Private Information. Delta Dental further breached these implied contracts by failing to comply with their promise to abide by HIPAA.

201. Additionally, Delta Dental breached the implied contracts with Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information they created, received, maintained, and transmitted, in violation of 45 CFR 164.306(a)(1).

202. Delta Dental also breached the implied contracts with Plaintiffs and Class Members by failing to implement technical policies and procedures for electronic systems that maintain electronic PHI to allow access only to those persons

or software programs that have been granted access rights, in violation of 45 CFR 164.312(a)(1).

203. Delta Dental further breached the implied contracts with Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 CFR 164.308(a)(1).

204. Delta Dental further breached the implied contracts with Plaintiffs and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii).

205. Delta Dental further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2).

206. Delta Dental further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3).

207. Delta Dental further breached the implied contracts with Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by their workforce violations, in violation of 45 CFR 164.306(a)(94).

208. Delta Dental further breached the implied contracts with Plaintiffs and Class Members by impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq*.

209. Delta Dental further breached the implied contracts with Plaintiffs and Class Members by failing to design, implement, and enforce policies and procedures establishing physical administrative safeguards to reasonably safeguard protected health information, in violation of 45 CFR 164.530(c).

210. Delta Dental further breached the implied contracts with Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' PHI.

211. A meeting of the minds occurred, as Plaintiffs and Class Members agreed, *inter alia*, to provide payment and/or accurate and complete Private Information to Delta Dental in exchange for Delta Dental's agreement to, *inter alia*, provide services that included protection of their highly sensitive Private Information.

212. Plaintiffs and Class Members have been damaged by Delta Dental's conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

COUNT IV
UNJUST ENRICHMENT/QUASI CONTRACT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

213. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

214. This Count is pleaded in the alternative to Counts II and III above.

215. Plaintiffs and Class Members conferred a benefit on Delta Dental by turning over their Private Information to Defendants and by paying for services that should have included cybersecurity protection to protect their Private Information. Plaintiffs and Class Members did not receive such protection.

216. Upon information and belief, Delta Dental funds their data security measures entirely from their general revenue, including from payments made to them by Plaintiffs and Class Members.

217. As such, a portion of the payments made by Plaintiffs and Class Members is to be used to provide a reasonable and adequate level of data security that is in compliance with applicable state and federal regulations and industry standards, and the amount of the portion of each payment made that is allocated to data security is known to Delta Dental.

218. Delta Dental has retained the benefits of their unlawful conduct, including the amounts of payment received from Plaintiffs and Class Members that should have been used for adequate cybersecurity practices that they failed to provide.

219. Delta Dental knew that Plaintiffs and Class Members conferred a benefit upon them, which Delta Dental accepted. Delta Dental profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes, while failing to use the payments they received for adequate data security measures that would have secured Plaintiffs' and Class Members' Private Information and prevented the Data Breach.

220. If Plaintiffs and Class Members had known that Delta Dental had not adequately secured their Private Information, they would not have agreed to provide such Private Information to Defendants.

221. Due to Delta Dental's conduct alleged herein, it would be unjust and inequitable under the circumstances for Delta Dental to be permitted to retain the benefit of their wrongful conduct.

222. As a direct and proximate result of Delta Dental's conduct, Plaintiffs and Class Members have suffered, and/or are at a continued, imminent risk of suffering, injury that includes but is not limited to the following: (i) the loss of the opportunity to control how their Private Information is used; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not

limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Delta Dental's possession and is subject to further unauthorized disclosures so long as Delta Dental fails to undertake appropriate and adequate measures to protect Private Information in their continued possession; and (vi) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

223. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from Delta Dental and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Delta Dental from their wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

224. Plaintiffs and Class Members may not have an adequate remedy at law against Delta Dental, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT V
CALIFORNIA'S CONFIDENTIALITY OF MEDICAL INFORMATION ACT
Cal. Civ. Code § 56, *et seq*.
(ON BEHALF OF PLAINTIFF LAMONS AND THE CALIFORNIA SUBCLASS)

225. Plaintiffs reallege and incorporate by reference the allegations contained in the preceding paragraphs as if fully set forth herein.

226. Defendants are "provider[s] of healthcare" services as defined in Cal. Civ. Code § 56.06 and are therefore subject to the requirements of the CMIA, Cal. Civ. Code §§ 56.10(a), (d) and (e), 56.36(b), 56.101(a) and (b).

227. Plaintiffs and the Class are "patients," as defined in CMIA, Cal. Civ. Code § 56.05(k) ("'Patient' means any natural person, whether or not still living, who received healthcare services from a provider of healthcare and to whom medical information pertains.").

228. Defendants disclosed "medical information," as defined in CMIA, Cal. Civ. Code § 56.05(j), to unauthorized persons without first obtaining consent, in violation of Cal. Civ. Code § 56.10(a). The disclosure of information to unauthorized individuals in the Data Breach resulted from the inactions of Defendants, including their failure to adequately implement sufficient data security and monitoring measures and protocols to protect Plaintiffs' and Class Members' Private Information, which allowed hackers to obtain such Information.

229. Specifically, Defendants' negligence resulted in the release of individually identifiable PHI pertaining to Plaintiffs and the Class to unauthorized cybercriminals and the breach of the confidentiality of that information. Defendants' negligent failure to maintain, preserve, store, abandon, destroy, and/or dispose of Plaintiffs' and Class Members' Private Information in a manner that preserved the confidentiality of the information contained therein is a violation of Cal. Civ. Code §§ 56.06 and 56.101(a).

230. Defendants' systems and protocols did not protect and preserve the integrity of electronic medical information belonging to Plaintiffs and the Class, in violation of Cal. Civ. Code § 56.101(b)(1)(A).

231. Plaintiffs and the Class were injured and have suffered damages, as described above, from Defendants' illegal disclosure and negligent acts and omissions resulting in the release of their medical information, in violation of Cal. Civ. Code §§ 56.10 and 56.101, and therefore seek relief under Civ. Code §§ 56.35 and 56.36, including actual damages, nominal statutory damages of $1,000, punitive damages of $3,000, injunctive relief, and attorney fees, expenses and costs.

COUNT VI
CALIFORNIA UNFAIR COMPETITION ACT
Cal. Bus. & Prof. Code §§ 17200, *et seq.*
(ON BEHALF OF PLAINTIFF LAMONS AND THE CALIFORNIA SUBCLASS)

232. Plaintiffs reallege and incorporate by reference the allegations contained in the preceding paragraphs as if fully set forth herein.

233. Plaintiff Kerry Lamons (for the purposes of this section, "Plaintiff") brings this claim on behalf of herself and the California Subclass.

234. Delta Dental is a "person" as defined by Cal. Bus. & Prof. Code § 17201.

235. Delta Dental violated Cal. Bus. & Prof. Code §§ 17200, et seq. ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

236. Delta Dental's "unfair" acts and practices include:

a. Delta Dental failed to implement and maintain reasonable security measures to protect Plaintiff's and California Subclass Members' Private Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

b. Delta Dental failed to identify foreseeable security risks, remediate identified security risks, and sufficiently improve security following previous cybersecurity incidents, as described herein. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiff and California Subclass Members, whose Private Information has been compromised;

c. Delta Dental's failure to implement and maintain reasonable security measures also was contrary to legislatively declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45, California's Consumer Records Act, Cal. Civ. Code § 1798.81.5, and California's Consumer Privacy Act, Cal. Civ. Code § 1798.100;

d. Delta Dental's failure to implement and maintain reasonable security measures also resulted in substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to

consumers or competition. Moreover, because consumers could not have known of Delta Dental's grossly inadequate security, consumers could not have reasonably avoided the harms that Delta Dental caused; and

e. Delta Dental engaged in unlawful business practices by violating Cal. Civ. Code § 1798.82.

237. Delta Dental has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), the FTC Act, 15 U.S.C. § 45, and California common law.

238. Delta Dental's unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and California Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff's and California Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that they did not properly secure Plaintiff's and California Subclass Members' Private Information;

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Consumer Privacy Act, Cal. Civ. Code §

1798.100, and California's Customer Records Act, Cal. Civ. Code § 1798.80, et seq., and § 1798.81.5, which was a direct and proximate cause of the Data Breach; and

h. Failing to provide the Notice of Data Breach required by Cal. Civ. Code § 1798.82(d)(1).

239. Delta Dental's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Delta Dental's data security and ability to protect the confidentiality of consumers' Private Information.

240. As a direct and proximate result of Delta Dental's unfair, unlawful, and fraudulent acts and practices, Plaintiff and California Subclass Members were injured and suffered monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for Delta Dental's services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

241. Delta Dental acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff's and California Subclass Members' rights.

242. Plaintiff and California Subclass Members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Delta Dental's unfair, unlawful, and fraudulent business practices or use of their Private Information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

COUNT VII
BREACH OF FIDUCIARY DUTY
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

243. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

244. In light of the special relationship between Delta Dental and their members, whereby Delta Dental became a guardian of Plaintiffs' and Class Members' Private Information (including highly sensitive, confidential, personal, and other PHI) Delta Dental was a fiduciary, created by their undertaking and guardianship of the Private Information, to act primarily for the benefit of their members, including Plaintiffs and Class Members. This benefit included (1) the safeguarding of Plaintiffs' and Class Members' Private Information; (2) timely notifying Plaintiffs and Class Members of the Data Breach; and (3) maintaining complete and accurate records of what and where Delta Dental's members' Private Information was and is stored.

245. Delta Dental had a fiduciary duty to act for the benefit of Plaintiffs and the Class upon matters within the scope of their members' relationship, to keep the Private Information secure.

246. Delta Dental breached their fiduciary duties to Plaintiffs and Class Members by failing to diligently investigate the Data Breach to determine the number of Class Members affected and notify them within a reasonable and practicable period of time.

247. Delta Dental breached their fiduciary duties to Plaintiffs and the Class by failing to protect their Private Information.

248. Delta Dental breached their fiduciary duties to Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic PHI Delta Dental created, received, maintained, and transmitted, in violation of 45 CFR 164.306(a)(1).

249. Delta Dental breached their fiduciary duties to Plaintiffs and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, in violation of 45 CFR 164.312(a)(1).

250. Delta Dental breached their fiduciary duties to Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 CFR 164.308(a)(1).

251. Delta Dental breached their fiduciary duties to Plaintiffs and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii).

252. Delta Dental breached their fiduciary duties to Plaintiffs and Class Members by failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI, in violation of 45 CFR 164.306(a)(2).

253. Delta Dental breached their fiduciary duties to Plaintiffs and Class Members by failing to protect against any reasonably-anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3).

254. Delta Dental breached their fiduciary duties to Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by their workforce, in violation of 45 CFR 164.306(a)(94).

255. Delta Dental breached their fiduciary duties to Plaintiffs and Class Members by impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

256. As a direct and proximate result of Delta Dental's breaches of their fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer the harms and injuries alleged herein, as well as anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT VIII
DECLARATORY JUDGMENT/INJUNCTIVE RELIEF (ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

257. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

258. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal and state laws and regulations described in this Complaint.

259. Delta Dental owes a duty of care to Plaintiffs and Class Members, which required it to adequately secure Plaintiffs' and Class Members' Private Information.

260. Delta Dental still possesses Private Information regarding Plaintiffs and Class Members.

261. Plaintiffs allege that Delta Dental's data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their Private Information and the risk remains that further compromises of their Private Information will occur in the future.

262. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Delta Dental owes a legal duty to secure their members' Private Information and to timely notify members of a data breach under the common law, HIPAA, and the FTCA;

b. Delta Dental's existing security measures do not comply with their explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect members' Private Information; and

c. Delta Dental continues to breach this legal duty by failing to employ reasonable measures to secure members' Private Information.

263. This Court should also issue corresponding prospective injunctive relief requiring Delta Dental to employ adequate security protocols consistent with legal and industry standards to protect members' Private Information, including the following:

a. Order Delta Dental to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

b. Order that, to comply with Defendants' explicit or implicit contractual obligations and duties of care, Delta Dental must implement and maintain reasonable security measures, including, but not limited to:

i. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Delta Dental's

systems on a periodic basis, and ordering Delta Dental to promptly correct any problems or issues detected by such third-party security auditors;

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training their security personnel regarding any new or modified procedures;

iv. segmenting their user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Delta Dental's systems;

v. conducting regular database scanning and security checks;

vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

vii. meaningfully educating their members about the threats they face with regard to the security of their Private Information, as well as the steps they should take to protect themselves.

264. If an injunction is not issued, Plaintiffs will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach at Delta Dental.

The risk of another such breach is real, immediate, and substantial. If another breach at Delta Dental occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

265. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to Delta Dental if an injunction is issued. Plaintiffs will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Delta Dental's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Delta Dental has a pre-existing legal obligation to employ such measures.

266. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at Delta Dental, thus preventing future injury to Plaintiffs and other members whose Private Information would be further compromised.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually, and on behalf of Plaintiff Robertson's minor children, and the Class described above, seek the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Nationwide Class and California Subclass requested herein;

b. Judgment in favor of Plaintiffs and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order instructing Delta Dental to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members;

e. An order requiring Delta Dental to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiffs and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

DATED: January 3, 2024.

Respectfully submitted,

By: */s/ Kyle McLean*

Kyle McLean (SBN #330580)
Email: kmclean@sirillp.com
Mason Barney*
Email: mbarney@sirillp.com
Tyler Bean*
Email: tbean@sirillp.com

SIRI & GLIMSTAD LLP
700 S. Flower Street, Ste. 1000
Los Angeles, CA 90017
Telephone: 213-376-3739

Attorneys for Plaintiff and the Proposed Class
**Pro Hac Vice Applications Forthcoming*